

Form PTO-	1449							ATTY DOCKET NO. APPLICATION NO NO						
INI	FORMA	IN A	AN	DISCI APPL	ICA	ATION	CITATION I	09/127,767						
						,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		Sarvar PATE & TRADEMINE						
								FILING DATE July 31, 1998 GROUP 2744						
U.S. PATENT DOCUMENTS														
EXAMINER INITIAL	D	OCUI	ME	NT NUM	BEF	₹	DATE	NAME	CLASS	SUB FILING DATE CLASS IF APPROPRIATE				
SK-	5	1	1 5 3 9 1 9			9	10/06/1992	Reeds, III et al.						
				<u> </u>					ļ					
: - : :						1	ODELCAL DATESTE F	OCH IMPENITIC	<u> </u>					
FOREIGN PATENT DOCUMENTS														
	D	OCUI	MEI	NT NUM	IBEF		DATE	COUNTRY	CLASS	SUB CLASS	YES	LATION NO		
									1					
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, etc.)														
	M. Bellare and P. Rogaway, Entity authentication and key distribution, Advances in Cryptology - Crypto, 1993.													
SK		S. Bellovin and M. Merritt, Encrypted key exchange: password-based protocols secure against dictionary attacks, <i>IEEE computer society symposium on research in security and privacy</i> , 72-84 May 1992.												
Ĺ		R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, and M. Yung, Systematic design of two-party authentication protocols, <i>Advances in Cryptology - Crypto</i> , 1991.												
	i	M. Blum and S. Micali, How to generate cryptographically strong sequences of pseudo random bits, SIAM J. Computing, 13 No. 4:850-864, 1984.												
		R. B. Boppana and R. Hirschfeld, Pseudorrandom generators and complexity classes, <i>Advances in Computing Research</i> , 5 (S. Micali, Ed.), JAI Press, CT.												
		U.S.	De	partment	of (	Commer	ce/N.I.S.T., Digital Si	ignature Standard, FIPS 18	6, May 1	994.				
		O. Goldreich and L. A. Levin, A hard-core predicate for all one way functions, <i>Proceedings of 21<sup>st</sup> STOC</i> , 25-32, 1989.												
		S. Goldwasser and A. Micali, Probabilistic encryption, Journal of Computer and Systems Science, 28: 270-299, 1984.												
		L. Gong, T. Lomas, R. Needham and J. Saltzer, Protecting poorly chosen secrets from guessing attacks, <i>IEEE Journal on Selected Areas in Communications</i> , 11(5): 648-656, June 1993.												
A		EIA	/TIA	, Cellul	ar Ra	adioTele	communications Inters	system Operations IS-41 Re	v. D, 199	97.				
EXAMINER	\				, 1	dal		DATE CONSIDERED						
	\sqrt	1	_2	KI	_			11/21/00			·			
EXAMINER: Initia applicant.	il if citation cons	idered, w	hether	or not citation	is in co	nformance wit	th M.P.E.P. 609; Draw line through c	itation if not in conformance and not considered	i. Include copy	of this form with I	next communica	ition to		

Sheet 2 of 3

Form PTO-	ORMAT	N AN	AF	PPL	ICA	ATION essary)		APPLICANT Sarvar PATEL FILING DATE July 31, 1998  APPLICATION NO 09/127,767  GROUP 2744					
	5 <u>-</u> 1						J.S. PATENT DO	CUMENTS				-	
EXAMINER INITIAL	DOC	UME	I TN	NUM	<b>IBER</b>	<b>t</b>	DATE	NAME	SUB CLASS		G DATE COPRIATE		
			<u>                                     </u>										
						I	OREIGN PATENT I	OCUMENTS					
	DOC	UME	NT I	NUM	<b>IBER</b>	t .	DATE	COUNTRY	CLASS	SUB CLASS	TRANS	LATION	
	<del></del>								ļ	<u> </u>	YES	NO	
		+-							-	<del> </del>	<del>  </del>		
		l		<u> </u>	000	IIID D	OCH PENTO		<u></u>				
SK	T. Lomas, L. Gong, J. Saltzer and R. Needham, Reducing Risks from Poorly Chosen Keys, Proceedings of the ACM Symposium on Operating System Principles, ACM Operating Systems Review, 23(5): 14-18, December 198  S. Patel, Information Leakage in Encrypted Key Exchange, Proceedings of DIMACS workshop on Network Three 38: 33-40, December 1996.  S. Patel, Number theoretic attacks on secure password schemes, IEEE symposium on security and privacy, 236-247, May 1997.												
	S. Patel, Weaknesses of the north american wireless authentication protocol, <i>IEEE Personal Communications</i> , 40-44, June 1997.											ຜ, 40-	
								ctions, Proceedings of 23 <sup>n</sup>					
	M. Beller, L. Chang and Y. Yacobi, Privacy and authentication on a portable communication system, <i>IEEE J. Selected Areas in Communications</i> , 11(6): 821-829, 1993.												
	C. Carroll, Y. Frankel and Y. Tsiounis, Efficient key distribution for slow computing devices: Achieving fast over the air activation for wireless systems, <i>IEEE symposium on security and privacy</i> , May 1998.												
	TIA/EIA Interim Standard, Over-the Air Service Provisioning of Mobile Stations in Spread Spectrum Systems, IS-683-A, June 1998.												
	E	Blos	som,	The	VPI	Protoco	ol for Voice Privacy D	evices, December 1996.		****	,	<del></del>	
		. Gold ryptol					and A. Micali, On the	cryptographic application	s of rando	m function	s, Advan	ces in	
$\bigvee$	D. Jablon, Strong Password-Only Authenticated Key Exchange, ACM SIG-COMM Computer Communications Review, October 1996.										ns		
EXAMINER  EXAMINER: Initial applicant.	Atra if citation considere	d, whethe	r or not	U/ citation	Sis in cor	M/	th M.P.E.P. 609; Draw line through c	DATE CONSIDERED  11 / 21 / 00  tation if not in conformance and not considen	ed. Include conv	of this form with r	ext communica	ation to	

IFORM PTO-		IN A	AN	API		'A'	TION	CITATION N	APPLICANT Sarvar PAT	APPLICANT Sarvar PATEL					
							U	J.S. PATENT D				<u>                                     </u>			
EXAMINER INITIAL	D	OCUI	MEI	NT N	UMBI	ER		DATE	NAME CLASS SUB FILING DATE CLASS IF APPROPRIATE						
						T					<u> </u>			•	
_															
							F	OREIGN PATENT	DOCUMENTS						
	DOCUMENT NUMBER							DATE	COUN	TRY	CLASS	SUB CLASS	TRANSLATION		
				Т		Т			:		<del> </del>		YES	NO	
		$\vdash$	-		+	+					-			<u> </u>	
<u></u>	<u> </u>	<u> </u>			0	TH	ER D	OCUMENTS (Includin	g Author, Title, Date, Pertine	ent Pages, etc.)	<u> </u>		<u> </u>		
		S. Li	ucks	, Ope				e: How to defeat di			voting pul	blic kevs. I	Proceedin	gs of	
	SK	the S	ecu	rity P	rotoco	1 V	Vorksh	op '97, 1997.				-			
	SK	Odeo for C	i Go Com	oldreic puting	ch, Sh g Mac	afi hin	Goldw ery, V	vasser, Silvio Micali ol. 33, No. 4, pp. 7	How to Construction, How to Construction, 92-807, October 1	t Random I 986.	Functions	, Journal o	f the Ass	ociation	
					-										
	<u> </u>														
	ļ														
									<del></del>				*******		
		-						· · · · · · · · · · · · · · · · · · ·							
									7			-		<del></del>	
		<del>                                     </del>			· · · · · ·										
EXAMINER	17		/	9 -	KI	1	11	/	DATE CONSIDER					<u> </u>	
EXAMINER: Initia applicant.	al if station cons	idered, wi	hether	or not cit	ation is in	confo	ormance wit	th M.P.E.P. 609; Draw line throug			I. Include copy	of this form with 1	next communica	tion to	

....: 1779